STRATEGIC DESIGN RESEARCH JOURNAL

Strategic Design Research Journal, 11(2): 65-78 May-August 2018
Unisinos – doi: 10.4013/sdrj.2018.112.03

Holding on to *dissensus*: Participatory interactions in security design

Claude P. R. Heath

claude.heath@rhul.ac.uk

University of London. Department of Mathematics. Information Security Group. Egham Hill, Egham, Surrey, TW20 0EX, United Kingdom.

Peter A. Hall

p.hall@csm.arts.ac.uk

University of the Arts London. Central Saint Martins. Graphic Communication Design Programme. Granary Building, 1 Granary Square, Kings Cross, London N1C 4AA, United Kingdom.

Lizzie Coles-Kemp

lizzie.coles-kemp@rhul.ac.uk

University of London. Royal Holloway. Department of Mathematics. Information Security Group. Egham Hill, Egham, Surrey, TW20 0EX, United Kingdom.

ABSTRACT

Recent high-profile cyber-attacks affecting the National Health Service (NHS) in the UK have brought into focus the fact that data, devices, and people are so intermingled that we now need a new way of approaching everyday security that provides an account of place. The assumption until now has been that the security of the individual will follow from technical security and that designing for security requires purely technological solutions. Our creative engagement method puts the human security of actors in the foreground, ensuring that actors who may ordinarily be marginalized may have their perspectives taken into account. The creative methods used include participatory physical modelling to co-design representations of what constitutes ontological security in the everyday for communities. LEGO and other materials allow participants to physically model matters of concern as tangible scenarios, using colored bricks to encode actors, infrastructure, and the movement of data. In this paper, a single LEGO model, depicting an internet-protocol home-banking service, is described in detail. A number of playful and agonistic interactions between our participants are examined through a place-based lens, using descriptive concepts from ontological and autonomous design, an approach designed to tease apart different aspects of our results. This reveals how a community constructs place, the perspectives and horizons of actors, and networks of resilience. We find that participants achieve positive insight into these scenarios by testing out the ways in which they can be broken down by antagonists and adversaries. Participants sustain a space of contestation in which dissensus is established and anticipation of breakdown can be played with.

Keywords: ontological design, autonomous design, ontological security, co-design, LEGO.

Introduction

Recent high-profile digital attacks like the ransomware Wannacry, which affected the National Health Service (NHS) in the UK last year (Ehrenfield, 2017), have brought into focus the fact that data, devices and people are so intermingled that we now need a new way of approaching security. The traditional approach has been that technical computer security is paramount (Hansen and Nissenbaum, 2009), and this is defined as 'protection against unwanted disclosure, modification, or destruction of data in a system and also the safeguarding of systems themselves' (CSTB, 1991, p. 2). Since the mid-1990s the study and practice of computer security has been dominated by the use of statistical or mathematical risk models, with research on this being funded at both national UK and European levels. The methods described in this paper developed out of one such initiative, and were designed to extend current forms of engagement with communities (TREsPASS, 2013-2017).

The assumption has most often been that the security of the individual will follow from technical security. However, there is also a clear practical and theoretical distinction to be made between the security of the data that is being shared across an infrastructure, and the ontological security of the actors who utilise technological services (Coles-Kemp and Hansen, 2017). This distinction is at the heart

of any thorough understanding of how the security of a person and of a community is enmeshed with the complex information-sharing environment. This information-sharing environment and the different levels of access to and control over its infrastructures, determines many of the opportunities available to communities throughout the world.

Current information security risk management methods do provide descriptive tools for assessing threats, most often through the systematic brainstorming of scenarios. One amongst many such approaches is to use the outcomes of brainstorming to create 'attack trees' (Schneier, 1999; ADTool, 2018; Figure 1). These are intended to show the steps an attacker might take to reach a goal, but the resulting diagrams very quickly become unwieldy, as with many of these approaches, with many branches and repetitions of 'leaves' (or steps) across the tree being added. In today's dynamic information-sharing landscape the process of making these trees is too slow, and is undermined by the imaginative human capability to create new lines of attack on-the-fly, even for multiple goals to be attacked simultaneously (Cropley, 2010; Mandal and Lim, 2008). Since the dominant discourses of information security are fixated on its potential impact on profit (Amoore, 2013), the focus is most often on the defence of an institution's assets rather than on the opening up of a space to decide the question of 'Security for whom?' This focuses on supporting the production of resilience through social practices, at either an organisational or community level.

This paper presents a creative co-design process for exploring a more expansive form of security in which the intersections between technological and individual security can be examined, and discuss the results obtained from these in a central case study concerning how to design security for a home banking system. The objective of the paper is to demonstrate how a dynamic and expansive approach to the design of security can be put into practice - through creative security engagements which are playful but also serious participatory research. In addition to this we suggest that our results can be successfully analysed through the lens of a number of interwoven concepts from democratic agonism (Mouffe, 2000, 2009), ontological design (Winograd and Flores, 1986) and autonomous design (Escobar, 2012, 2017), with a view to supporting diverse cultures and perspectives by helping to make them stronger in a technologically mediated world. Within this, a place-based modelling lens composed of the following three intersecting points of interest stand out as being intrinsically connected to participatory modelling with particular communities. This will help us to see the connection between physical modelling and how communities can protect themselves by creating a clearer picture of what resilience means to them.

(i) The concept of developing *place-based ontologies*, with physical modelling, which can be used to inflect subsequent work to secure the kinds of relationships that exist between actors, and how this can include and centralise actors that might otherwise be marginalised through the use of traditional approaches, such as the attack tree.

(ii) The *perspectives and horizons of actors*, and of the reshaping of these horizons, is a means of designing technical security structures that contribute to resilience as defined by a community. Agonistic but playful interactions during physical modelling support the everyday life of communities, through the representation and discussion of everyday identities and perspectives emerging out of this. These represent what 'constitutive difference' is for a community (Staten, 1986): specifically, determining who is on the 'inside' and who is on the 'outside'. This can be seen as a natural extension of place-based modelling.

(iii) Physical modelling elicits *networks of resilience*, working with a community's natural strengths, especially where modelling shows how breakdowns in practices can be planned for and avoided by building on inherent community resilience.

These three topics are brought into the discussion of our results to illustrate how they can be used to analyse participatory modelling. Our aim here is not to instrumentalise ideas from ontological design and autonomous design or to construct a rigorous framework, but to test out just a few points of connection between these ideas and conventional technical security design- in order to broaden the range of possibilities for supporting the resilience of communities of different kinds.

We hope that by describing our results in some detail, and by including excerpts from participant speech, that this will bring to life the above three areas of interest, showing the aptness of these concepts to the analysis of participatory design and co-design data: how they have been enacted by participants through the media of physical modelling and diagramming. We also point to the importance of contestation and agonism as a necessary and sometimes desirable aspect of the co-design process.

Related work

Anthropologist Arturo Escobar introduces the concept of 'autonomous design' to describe the potential of a traditional and marginalised community to 'practice the design of itself' (Escobar, 2017, p. 5). While the subjects of information security are not conventionally considered traditional or marginalised, we contend here that a creative approach to security considers those whose ontological security is threatened by cyber and physical attacks, hacks and other breaches: be they refugees relying on mobile phones or small businesses relying on micro-loans administered through IPTV (internet protocol television). In creative security, as we call it, the discourse of situated knowledge and practices (Haraway, 1988) is an essential starting position, so that information security can be addressed in a non-abstracted way by considering the effects of place and space.

Escobar describes autonomous design as requiring 'a different sort of attitude that comes from dwelling in a place and from a commitment to a community with which we engage in pragmatic activity around a shared concern, or around a 'disharmony", through 'intense engagement and involved experimentation' (Escobar, 2012, p. 36). A typical line of investigation in this approach, he says, is to ask,

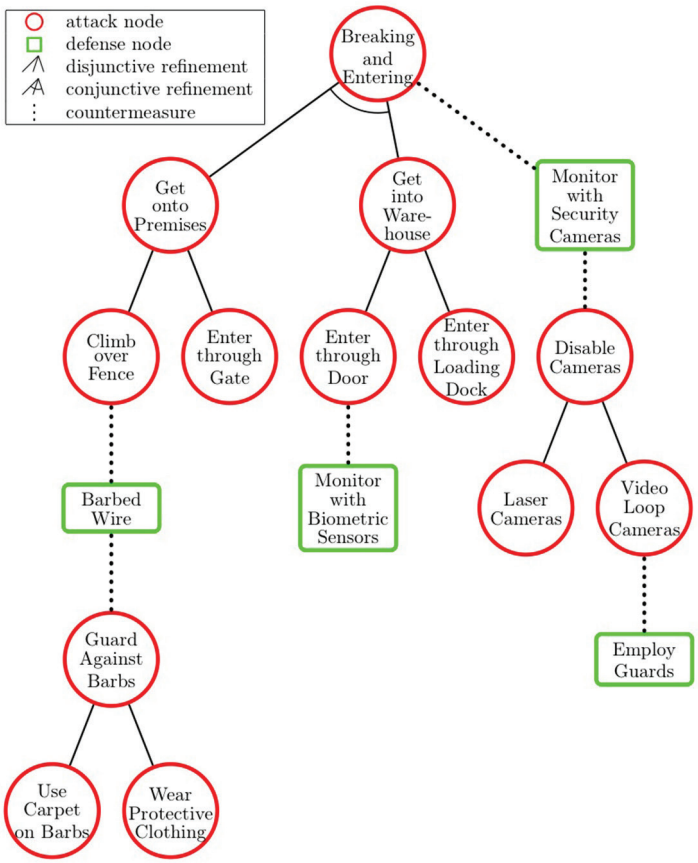

Figure 1. An 'attack tree', generated automatically by ADTool on TREsPASS. This is a relatively simple demonstration example, while others may run into the hundreds of 'branches' and 'leaves'. The goal of the attacker is at the top of the tree: 'breaking and entering'.

"Why do we/I see this as a problem?' and to follow each 'because...' with another 'why' until participants' values are made explicit' (p. 47). Such open-ended conversations, he notes, 'often go on for hours seemingly without a concrete agenda. Planners miss this dynamic altogether, or consider it inefficient or even a waste of time' (p. 47). However, out of this, a 'model' of 'the problem at hand' is produced, and: 'The concrete result is a series of tasks, organizational designs, and criteria by which to assess the performance of the system' (p. 47). For the participating community, this creates 'a learning system about itself' (p. 46), where they design criteria that emphasize 'place-building, relocalisation, renewed attention to materiality' (p. 8), resulting in 'changes in the horizon that shapes understanding' (Escobar, 2012, p. 38).

In participatory design research, diverse shared spaces of contestation using artefacts are crafted, and the status of these is debated in the literature. Binder et al promote the concept of 'design things', "things' that gather human being together' (Binder *et al.*, 2011, p. 6). Björgvinsson describes how 'agonistic thinging' with a 'polyphony of voices' reveals the ways in which public spaces have been hegemonically 'striated' for participants, and ask whether it is indeed possible to attain 'a sustainable agonistic space' (Björgvinsson *et al.*, 2012, p. 143). Hillgren *et al.* note that spaces of 'agonistic infrastructuring' need to be supported through 'strategic design to ensure that the claims and voices of marginal actors can grow stronger' (Hillgren *et al.*, 2016, p. 96-97). For DiSalvo's GrowBot participants, 'politics were actively projected onto and through artifacts', through a dialogic process of 'critical making' that highlights the possibility of a public and 'hybrid' practice respecting the desired and 'perceived politics of artifacts' for different publics (DiSalvo, 2014, p. 104). This can be seen as a key aspect of 'adversarial design', 'a condition of forever looping contestation' in which objects and 'spaces of confrontation' and 'spaces of contest' are provided as a resource for democratic pluralism (DiSalvo, 2012, p. 5; 2010. p. 4). Keshavarz and Mazé address 'the problematics of relating to 'others'', by querying 'the framing and staging of relations among diverse participants, including those with very different starting points than designers' (Keshavarz and Mazé, 2013, p. 8). In doing so they make use of Jacque Rancière's notion of 'dissensus', which, as they describe, 'concerns a break in the sensible order, [...] in which the established framework of perception, thought and action is confronted with the 'inadmissible'' (p. 11). It is via these breaks, they say, that the distributed 'times/spaces of contemporary practices' can be accessed. These are difficult to elicit in participatory design, they say, but it is around this that a 'dissensual community' can be established (p. 23). Working with the breakdowns of everyday patterns, rather than against them, is central to ontological design. In this case the 'domains of anticipation' within a community are clearly revealed by

failures occurring within the particular space of 'possible breakdowns' afforded by those domains (Winograd and Flores, 1986, p. 69). For the purposes of gaining insight into how a community conceives of and designs itself, Winograd and Flores, as well as Escobar, insist that 'a breakdown is not something negative' (Escobar, 2012, p. 38).

Methods: creative security engagement

Creative security engagements are founded on four principles: they are playful, participative, open-ended and democratic (Dunphy *et al.*, 2014). Moreover, they are designed to support and structure conversations about digital security, and to function as a vehicle to bring the perspectives of communities to different organisations and to government (Heath and Coles-Kemp, 2017). This includes any relevant tacit or previously unshared knowledge that stakeholders may possess, ensuring that their perspective is clearly identified and sufficiently built into any later work. Our methods contrast with but can also be used, if desired, in conjunction with other more structured and conventional approaches such as interviews, focus groups, and questionnaires. In contrast to the method described below, the official 'LEGO Serious Play' methodology is highly structured and requires participants to work individually at the outset, after which shared group work takes place (Cantoni *et al.*, 2011). Variants of the methodology have been used in organisational strategic planning, and in gathering requirements for design more generally (Bürgi and Roos, 2003; Roos *et al.*, 2004; Schulz and Geithner, 2011).

Research rationale

Our engagement method creates safe spaces where people can share their matters of concern, air differences without hindrance or fear of consequences, and has been evolved through trial and error and with participant feedback. Creative security methods encourage people to reflect on their environment, the emotions they feel, the constraints they experience, the pressures that they undergo as well as the actions and the tasks that they perform when generating and sharing information. The methods encourage the use of colour, imagery, shapes, textures and sound as well as text to reflect upon and articulate the situations in which information is generated and shared. By encouraging this broader type of thinking, security issues are also articulated from the perspectives of different groups within a context. The method seeks to identify how groups currently respond to those issues, enabling digital and other security strategies to be developed that respond to these wider issues while promoting and working with the strengths of the groups.

In the context of information security, physical modelling occupies a space between the typical diagrams (flow-charts and UML diagrams for example) that security practitioners commonly work with, and the everyday practices of those who are affected by security design. LEGO in particular provides a physical method where modularity and connectivity bridges this space very effectively. LEGO models become richly decorated with mini-figures, annotations, connections of different kinds between elements, and fantastical structures, evocative of security in the everyday for our participants. We see this as an extension and a democratisation of the traditional risk assessment process, enabling fundamental questions to be addressed by participants, such as 'whose security are we talking about?' The conversation around these questions is moved forward by participation in (and through) the joint modelling process described below.

Research methodology

The research methodology is as follows:

(1) *Session structure and presentation.* Pre-meeting and briefing sessions are followed by one or more initial hands-on sessions in which different materials are used with the group to advance the discussion of the core concerns and values of the group. These sessions test the appropriateness of different materials. Participatory diagramming (Figure 2) and modelling using a variety of materials (Figure 3) are introduced, familiarising the group with the process of working through their concerns using shared means. This also identifies the values that can be looked at together during later stages of the engagement process.

During this first phase, participants have the opportunity to make joint diagrams on paper, demarcating particular areas and questions to be addressed in the subsequent physical modelling. Our introductory remarks often ask participants to respond to a design provocation as a starting point for the diagramming discussions. After this narrowing down of interest onto specific topics and questions, we ask participants to divide themselves into subgroups of between three and six people, and invite them to consider the particular scenario they have in mind in more detail. LEGO kits are provided to them, including grey LEGO base-boards to build upon. An optional colour code to use with the bricks is supplied (Figure 4). The colour scheme for this is: data (blue bricks); infrastructure (green); and actors (yellow). This colour scheme is loosely based upon a schema developed by the Open Group for graphically modelling business enterprises (the Archimate tool, Lankhorst *et al.*, 2009). The groups are encouraged to develop their own schemas on the back of this, or in entirely new ways, to assist in modelling the kind of situations they intend to look at.

The physical modelling session is structured by allocating different roles to group members. Each group is self-facilitating to a great extent. Participants volunteer for suggested roles: (1) the scribe, who annotates and documents the group discussions and the rationale behind particular modelling decisions; and (2) the narrator, who towards the end of the session presents the narrative of the model to the wider group. The scribe can also use an open source online app that we have designed for the purpose of summarising models graphically (InterActor, 2018). Participants are not asked to diagram and model all of the possible dimensions of a given scenario. Only the most salient features are modelled, that is, those considered to be the most relevant by the groups themselves. If applicable, the groups are able to envisage not only how things are in a present scenario, but how they could be imagined in a desired future state of affairs.

An overview and synopsis phase follows the model-building. Each of the groups takes a turn to make a short presentation of the information-sharing and protection narratives that emerged when making their model. This is an opportunity for participants to re-examine their self-defined starting questions. After this, and towards the very end of the session, groups are invited to merge all of the models from the different groups, arranging them in such a way that the separate narratives are able to resonate with one another. This allows for participants to gain a new perspective on their work: the generally consistent format of the models, plus the common starting points, serves to highlight the connections and differences between the outputs of the different groups.

(2) *Data gathering.* Initially, a selection of materials is provided to participants, including pens and large paper sheets, with which they can map their first response to a provocation. After a short time, the LEGO kit is given to them, which also includes a number of small blank cards and pens, with which to annotate their models. This is as well as adhesive tapes, strings, and other means of augmenting the models. Sessions are audio- and video-recorded, and photographs are made of the diagrams, the LEGO models, and each group's notes. This documentation also includes the verbal presentation of the model to other groups, and the merging and overview segment of the session.

(3) *Data analysis.* An open source audiovisual transcription package is used to create an annotated transcript of participant speech, and to map this to physical spaces in the models (ELAN, 2017; Figure 5). In parallel with this, and in order to overcome the difficulty participants might have in reworking their constructions in the time available, digital collages are made of the LEGO models (Figure 7). This preserves the appearance and desired spatial relationships between the built items, but separates the flows of information and actor relationships, so that the overall pattern may be seen more easily. A list of ranked keywords is then generated through a corpus analysis of the transcript (AntConc, 2013). Positive or negative keywords are extracted from this (using the Brown corpus as reference). This shorter list of positive and negative keywords is then cross-referenced with the physical points of the LEGO model referred to by speech. By linking keywords to the spaces and places of the model, a heat map view of the scenario can be created (Figure 8). This maps out the key topics connected to the security and wellbeing of the community being modelled.

(4) *Reporting*. In a post-event report the separate and combined group narratives are represented concisely, and this includes photographs, sometimes taken by the group members themselves. This report is shared with the group by email, or in paper form, as soon after the session as possible. Any feedback that is received from the group on this, is then incorporated into a final version of the report for sharing with the relevant stakeholders and beyond, if the engagement requires.

Figure 2. Initial sessions use shared diagramming to map out the prime areas of responsibility and concern for different participants. These outputs are later fed back to the group as a set of design principles, and as target graphs showing how their responsibilities and concerns map onto each other.

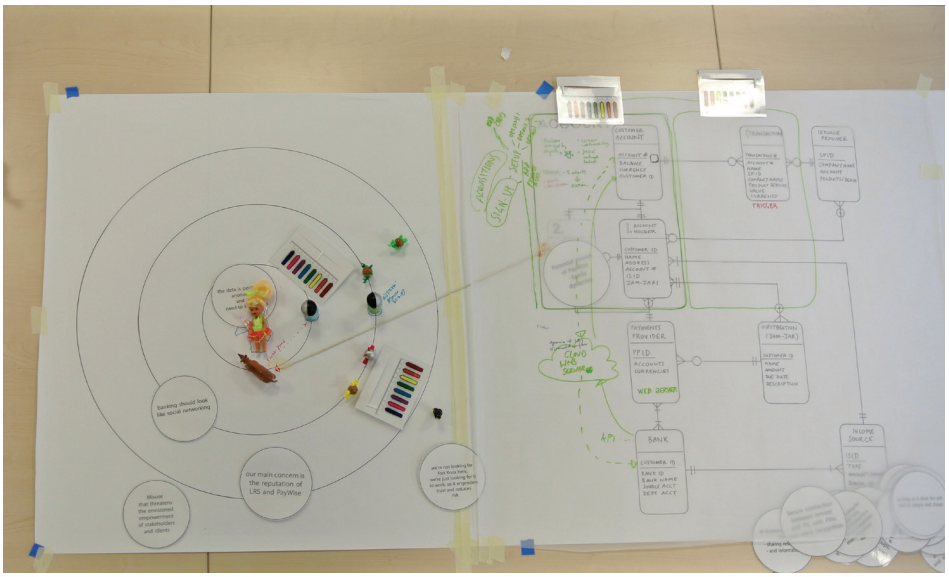

Figure 3. Follow-up sessions employ a mix of materials to narrow the field of enquiry with regard to the groups' developing projects. Here the target diagrams of core values and concerns are populated with various toy avatars, the distribution of which is cross-referenced with an enlarged hand-drawn technical diagram of the service as supplied by the group.

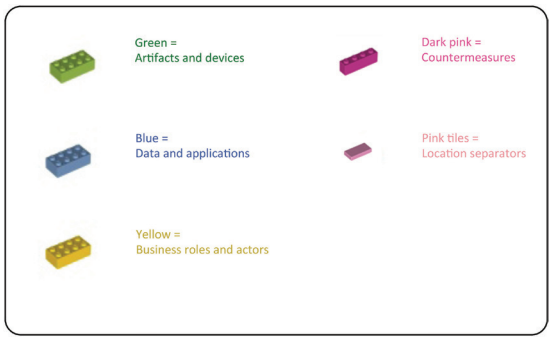

Figure 4. The LEGO colour schema. This is provided to participants as a suggested way to encode the movement of shared information. Some groups go on to devise schemas of their own.

Results

This case study, with a small London-based social enterprise, looked at how a new home-banking service for people in local communities on low incomes could be launched using an internet protocol television (IPTV) infrastructure in their homes. Our aim was to help the different stakeholders involved in the design, provision and use of the service to discuss whether there might be other ways to define the service. The briefing for this case study established a motivating factor to provide access to banking for older members of communities who distrust online transactions, and who may not own computers or smart devices.

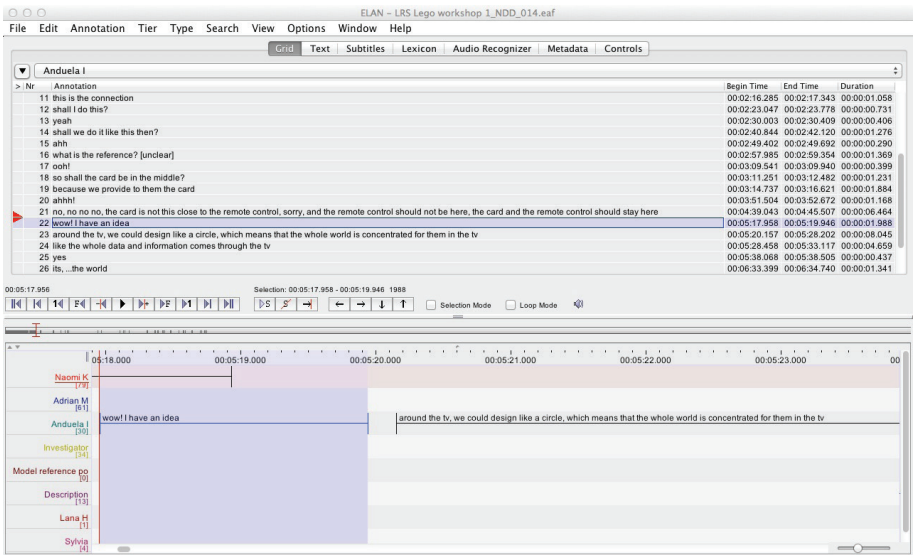

Figure 5. The ELAN coding of the IPTV model. The annotations on some layers (or tiers) refer to conversational topics raised within the group. These were later used to generate graphical heat maps over the digitally collaged re-mapping of the original LEGO model.

Our participants were members of the service design team who wished to scope the security of the service, prior to running focus groups with users in the communities they served. They were initially shown box diagrams and flow charts representing the technical layout of the service, but the participants failed to recognise themselves in these technical representations (despite having provided a number of these to us). Our discussions stalled due to the difficulty of relating these representations to their core business values and to the motivating vision of the staff and managers. After initial trials using mixed hand-drawn diagrams and toys for avatars (Figure 3), LEGO was introduced with more successful outcomes. Six participants were able to model in LEGO the home of the typical service user, and to refine their understanding of how data should be allowed to enter and leave the home, as it flowed across the IPTV service (Figure 6). In a follow-up up session the same group discussed and refined the same model in consultation with our team. They were able to shape the different protections required for the service to maintain its integrity and relevance for the communities in question. In terms of the instrumental requirements of security-design, the modelling process resulted in the following insights:

(i) The process enabled the participants to scope the implications of particular combinations of technology, with a view to making it feel familiar to users (AMP smart plugs, televisions and remote controls).

(ii) Participants were able to specify the correct levels of encryption needed for financial data in movement and at rest, at different points along the transaction pathway, and across the banking system and cloud provider. This was discussed as a mix of data redaction, unique identifier codes, and encryption at different places in the model.

(iii) The group was able to clarify the organisational position that the client should own data emerging from use of the system, and worked through a number of ways in which the system architecture design should support this. Participants were able to scope and test criteria for context-sensitive ring-fencing of different areas of the service, with business rules for defining what an alert is and at what level it can be declared. These might be alerts relating to overspending, unusual data patterns and energy use, in conjunction with local health and social services. Participant AM noted the system should require that 'to become an alert we have to notice the interest and concern of at least five different professionals in a particular family'; 'to protect people from false alerts', and 'so, trigger an intervention... [even though] you're not sharing any user data.' The modelling helped to clarify how to avoid the risk of data interception and modification, tampering and other forms of unauthorised access.

(iv) Participants were able to specify that the system can accommodate carers and relatives being given permissioned access to the data under certain conditions and for certain purposes.

(v) Participants were able to make plans for team debriefing after 'human' interventions (where a partner organisation sends a trained worker to visit the family and enquire as to their wellbeing and identify why an overspend has occurred, for example). This precaution is especially necessary for the removal of data 'puddles' left behind after releasing data following an alert that has been actioned in such a way.

(vi) It was also concluded that a new 'Troubleshooter' role should be created to field specific data requests and manage how alerts are handled by the five service partners. Subsequently, new Archimate models were generated as a result of the above insights, and a digital collage of the model (Figure 7) was given as part of our feedback to the participants. Finally, a heat map of the positive and negative sentiment around the service was made using the methods described in the previous section (Figure 8).

Place-based modelling

Aside from the instrumental or pragmatic outcomes mentioned above, how can our results be described in terms of the place-based modelling lens described in the Introduction? LEGO modelling is place-based in the sense that a localised ecology is created around a recognisable and tangible scenario derived from a communities' everyday reality. Actors are naturally situated in a model amongst an array of other items (infrastructure, data, roles, and anything else they wish to incorporate). These actors then animate a complex and hybridised physical-digital space.

In the IPTV model, the home is differentiated by having a relatively high degree of internal structure (Figure 9). Elements are built around the remote control and the television, used by the tenant to manage her money. On either side are her two children. The television is very large in comparison, due to its stated prominence in the life of the family. The area around the television has been given a ring of green stem-like pieces that represent the homes' active 'connectivity' to the outside world – the access to information provided via the television:

P1: wow! I have an idea
P1: around the tv, we could design like a circle, which means that the whole world is concentrated for them in the tv
P1: like the whole data and information comes through the tv
P2: huh!
P3: ok
P2: which it sort of does! [...]
P1: ohh, oh, now this is their world
P3: this is interesting, that this is their world, like that, i-it could either be that, or, it could be a PC or whatever
P2: it could, yes
P3: as everyone has a PC, w-w- , as everyone has
P1: like in a circle like this
P2: and what is it?
P1: its, ...the world

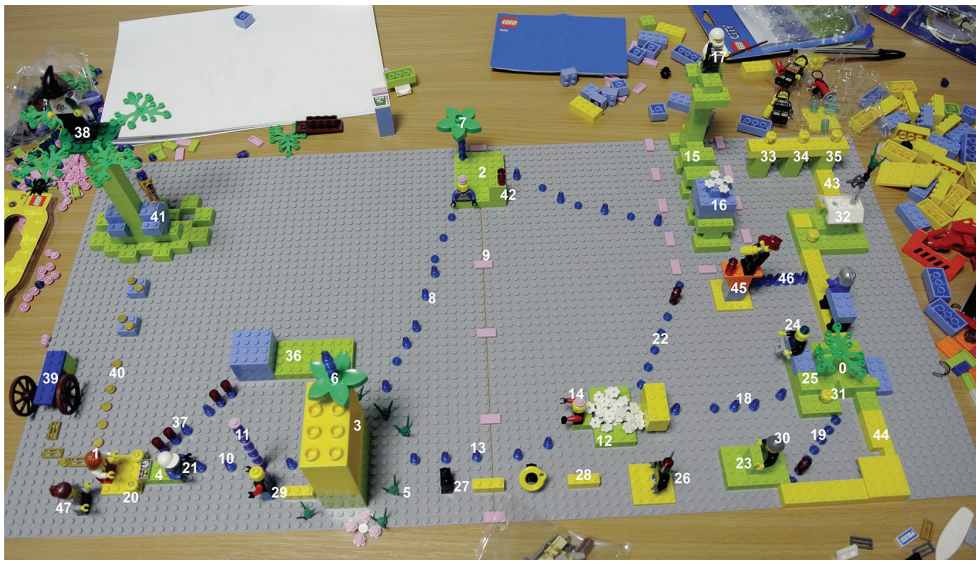

Figure 6. The IPTV service design LEGO model. Key: 0 = Service Provider; 1 = Client; 2 = Card; 3 = TV; 4 = Remote; 5 = Client's sphere of interest; 6 = Antenna on TV; 7 = Antenna on Card; 8 = Data TV to Card; 9 = Boundary between Client and Service Provider; 10 = Data Remote to TV; 11 = Raspberry Pi; 12 = Cloud; 13 = Data TV to Cloud; 14 = Protection on Cloud; 15 = Bank; 16 = Account; 17 = Security on Bank; 18 = Data Cloud to Service Provider; 19 = Data Service Provider to Partner 23; 20 = Children; 21 = Security on Remote; 22 = Data Bank to Cloud; 23 = Partner 23; 24 = Service Provider Data management; 25 = Service Provider Server; 26 = Partner 26; 27 = Intervention in progress; 28 = Intervention pathway; 29 = Partner 29; 30 = Staff at Partner 23; 31 = Staff at Service Provider; 32 = Partner HA; 33 = Partner 33; 34 = Partner 34; 35 = Partner 35; 36 = Energy provider; 37 = Data Bill to Client; 38= Governmental welfare agencies; 39 = Income source; 40 = Welfare benefits; 41 = Government systems; 42 = Additional cards; 43 = Partner bridges 1; 44 = Partner bridges 2; 45 = Troubleshooter; 46 = Data Troubleshooter to Partners; 47 = Carer.

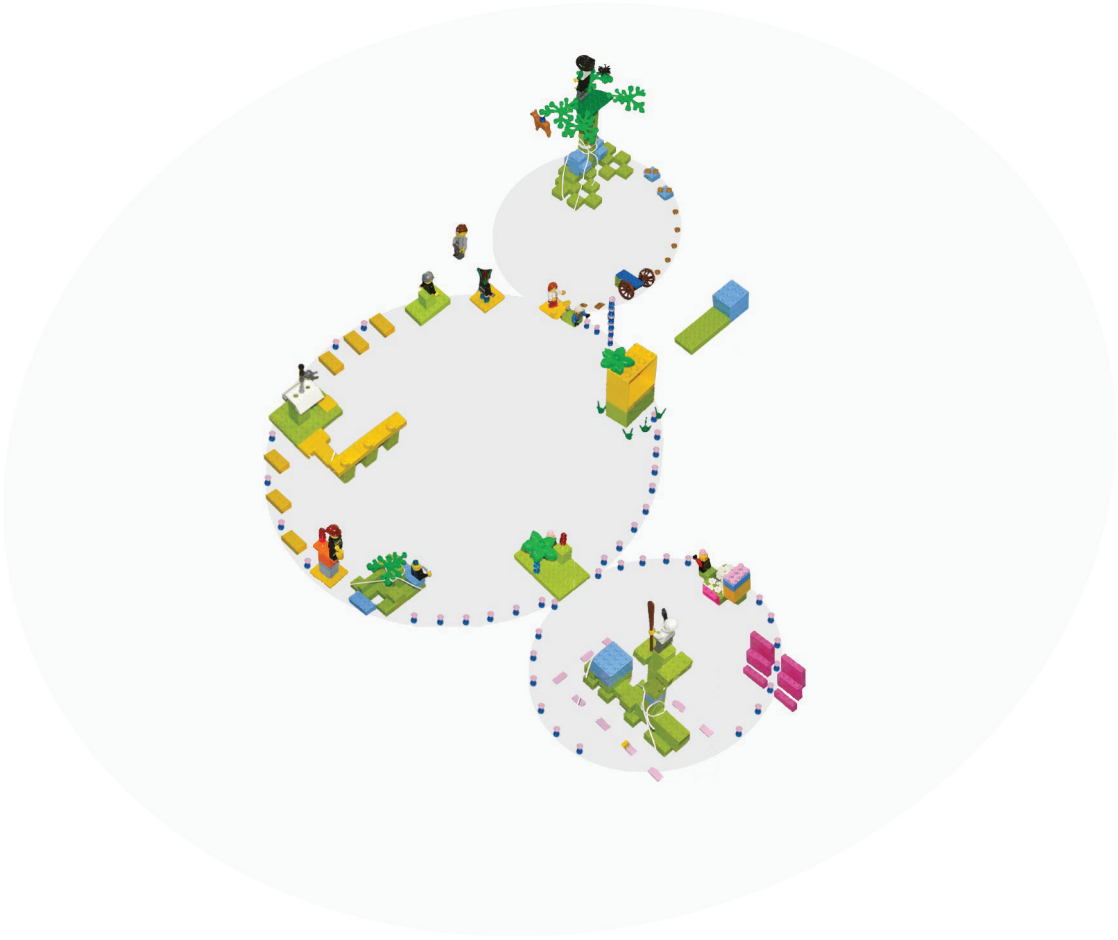

Figure 7. As part of our reporting to the participants, a digital collage was made from photographs of the original IPTV LEGO model. The elements of the model were grouped according to the functions and processes assigned to them by the group, aligning at specified points, to form an overview of the relational service design.

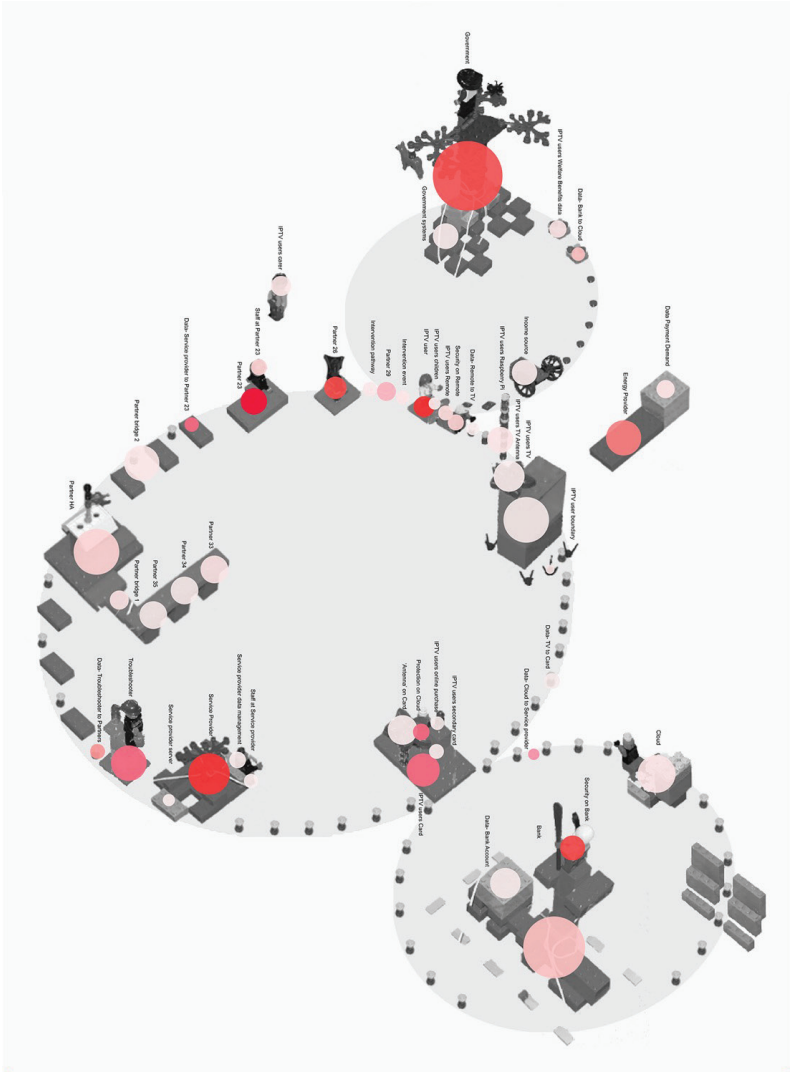

Figure 8. The IPTV model collage has a heat map superimposed over it, based upon positive and negative keywords found in the recordings of the speech of participants. The size of the circular nodes denotes the number of mentions of this part of the collage, and increasing red colour denotes the frequency of negative keywords at this point in the model.

Data from the family then flows out into the service infrastructure more widely, looping over to the banking platform and to the service provider partnership, via the cloud provider service. The modelling process is grounded in the construction of differentiated spaces and locations of the participants' own devising, gradually building up a representation of how the community sees itself within this scenario. The ring of green antennae are place-holders - for the core of the family's activities in connection with this home-banking service. The green ring also sets this zone apart, marking it out as the safe space for the family. It can be argued that the green ring added to the home by the group is a tangible 'field inscription' of shared space (Heath, 2014). This is a field constructed by the participants, which can be made visible with line drawings and is an analysis of shared space which can be supported by their speech (Heath *et al.*, 2014). In this case the participants have used the green ring of LEGO to help delineate the qualitative as well as the logical limits of the home.

The separateness of the home, as compared to other locations, is clear when viewing the model from the vantage point of the home, as for example when the tall light-green structure representing the government looms over the home from a distance away (Figure 10):

P1: and this was my idea, this is their world, and this is the antenna because they get all the information, via TV
P3: it's their whole world, that's why the TV is so big
P1: and this is the door
P1: accessible from
P2: I've got slightly worried about having said that this is their whole world, because I'm not convinced that that's really fair, but
P3: [unclear]
Investigator: it's their connection to, the whole world?
P2: yeah, it's their door to the outside world

The group took great care to model the potential effects of its proposed IPTV service on clients, as described at the beginning of this section (effects that can be both intended and unintended). By working through the impli-

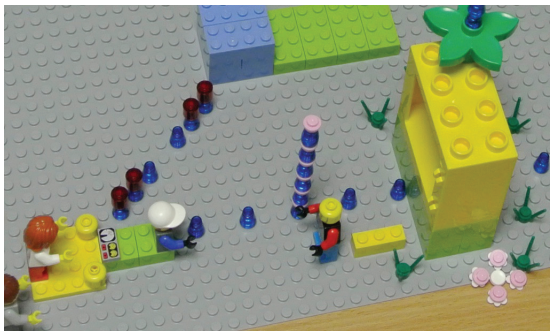

Figure 9. The service user (with red hair at bottom left) is in her home. A carer is behind her, and her two children are immediately in front of her. In front of them is the remote control with an avatar representing the security controls on the remote. Small blue data bricks flow out from the remote towards the large yellow television (via a 'Raspberry Pi' chip with stack of blue data and pink controls). The diagonal line of blue data with red alerts placed on them represents the arrival of a large payment demand from a utility company, which sparks the overspending of the client and leads to a soft intervention visit from a specialised partner worker. The area around the television was given a ring of small green plant-like pieces that represented the homes' active 'connectivity' to the outside world.

cations of the user's perspective and those of other actors - including that of the service partnership, of the bank, and of the government - they produced a new 'horizon of understanding', a hybrid of all of these perspectives and of their own as the service providers. These perspectives were then integrated into a revised approach to the design. This process centred on ensuring that unintended consequences for the client would not compromise their 'door to the outside world', and destroy the credibility of the service. Reflecting on the session afterwards, participant NK stated: 'The best thing about this is that normally we have to try to somehow keep all of this in the mind, whereas this [process] allows us to see it all at once.' This comment suggests that a strategically significant new view of the home and its' relevant horizons had been gained through the participatory physical modelling process.

The speech accompanying the modelling reveals how the groups constructs different varieties of the 'constitutive other' (Staten, 1986). The abstracted and remote structures of the bank and government, which have a degree of internal differentiation based on known functionality of those institutions but little spatial differentiation, and are in marked contrast with the detailed 'place' which is the user's home. For other actors such as attackers, about whom little is known due to their being truly 'other', no representations of infrastructure or data have been added to the model. These are dematerialized actors - with no physical presence on the board. The properties of potential attackers on the service are discussed by participants in a fabulatory vein:

P1: Did you see the hacker, up there?
P4: yes, huh
P5: no this is the hacker, and this is the dog trying to be security
P3: hacker, no, that's absolutely important, because hackers threaten absolutely everybody
P1: because actually the hacker is not in [us], this is [us] isn't it?
P3: outside, yes

Figure 10. The actors in the home, the parent (user) and carer (with brown hair) face towards the children and television (out of shot at right). To one side and not in their immediate vision is the tall green tower representing the government, with a witch-hatted figure aloft, and green 'tentacles' spreading outwards. A dog is suspended there to suggest the possibility of teeth, of being bitten by government. Blue data is piled at the towers' base, and a trickle of intermixed blue data and gold coins (money) moves towards the home. The square block of blue which is the energy payment demand is encroaching into the home space.

P1: but the hackers are everywhere, y'know, by definition
P4: they're flying, huhah over, huh huh
P1: but then it looks like, haha, Santa Claus
P1: it flies, the hacker flies!

The group also debated how to represent the high street bank holding the customer's data and controlling the release of her funds. It is a green and blue towered construct, with a figure on top wearing a white helmet and brandishing a long weapon-like implement (Figure 11). Reversing conventional expectations, the bank takes on the appearance of an adversary, revealing it to be a potential area of agonistic interaction for the user of the IPTV service. If not managed effectively, the bank's communications with the service provider partnership - including alerts raised by the client overspending - could impact on the clients' rented housing situation and their access to government benefits:

P3: I'm going to put
P3: Visa, American Express thing on there
P3: and then we need to put the customer account on there don't we

P3: this is the huge bank at the heart of the economy
P2: and also, it's, it's quite threatening
P6: I think that should be lower, haha, it's too, it's too, imposing

By constructing actors with differing degrees of closeness to the home and differing degrees of threat to the home, the participants were able to track a number of the possible intended and unintended consequences of the service design. It is noteworthy that the participants preferred to track the performance of the service through this kind of relationship, rather than via any relationship to an attacker. There were different roles to be played by adversaries and by the more supportive actors - the latter primarily relates to actors such as the service partnership, who see themselves as being there 'to stop small problems becoming big ones' for their users. At a briefing meeting, staff described their vision of themselves as a social enterprise and 'a trusted data aggregator', saying that 'banking should look like social networking'. They wished to deploy a system 'where data is only exploited for the benefit of those who own it', that is, the users. This is in contrast to the attacker described above, an actor that does not share any common ground with any of the other actors in the model, contested or otherwise. The attacker is a fully fledged (if also dematerialised) antagonist as opposed to an adversary with whom there is some common ground.

Having seen how place and actors have been constructed in shared modelling using LEGO, we can now turn our attention to the ability of this method to depict recurring and abstracted patterns running through the models. This specifically relates to how human practices are mapped onto different places within models using concepts of time and space. The group consider the scenario previously mentioned, where the user is made homeless through an unintended consequence of data management, and they run this through the different facets of their model in order to see how this might unfold. The participants discussed how this outcome could be avoided:

P2: you know, how you, I hadn't really thought about that as a collaborative early warning system
P2: person could become homeless and wouldn't have a [bank] card either
P3: we're talking about fraud, abuse, loss of the card, abuse from within the family
P2: it can still happen, so what happens here if that happens?
P3: who is then responsible?
P2: will there be
P2: trigger, action, which can put in place all of the services which are nothing to do with us
P3: it's the early intervention that people want, the alerts [...]
P2: troubleshooter
P2: but that's an interesting point, we have an Account meeting on Monday, so I think I'll raise it

The group finds that an extreme but possible breakdown scenario reveals the need for a new 'Troubleshooter' role to be created, whose purpose is to manage the way in which that data is handled across the service. In creating a new business role the group has effected a change in the proposed design, and it has also evolved a new domain of anticipation with which to envisage further 'spaces of possible breakdown', (as Winograd and Flores call them), all over again. Far from being a problem, this is seen as a positive outcome from the modelling process, as it advances the design to a new level of insight. There has been a reshaping of the horizon embedded in the model, and the reflexive inter-

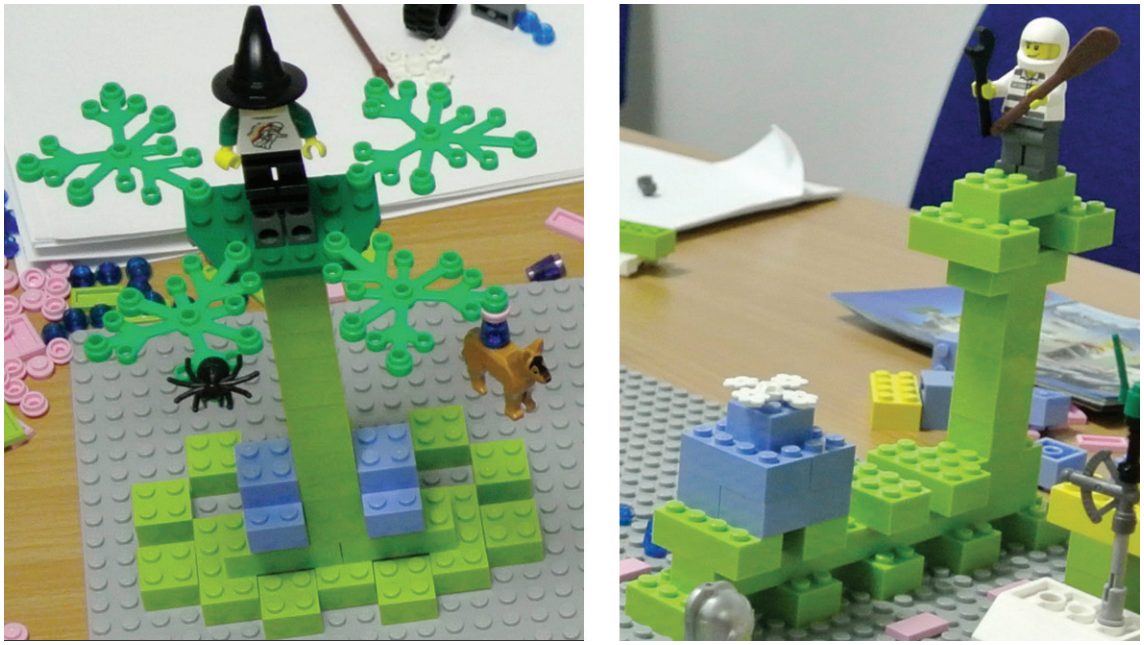

Figure 11. Left: the representation of the government- see previous image for full description. Right: the 'imposing' banking platform, with figure on top representing the security and controls within the banks sphere, demarcated by a rectangle made of pink tiles, as per the colour schema for location' provided to participants.

action with the model requires changes to be made in the elements they have previously built. The group has arrived at a new interpretation of the possible spatial and temporal patterns of the model, and this shows how LEGO can successfully be used to manage the interconnectedness and changeability of place and horizon within a scenario.

Discussion

Having examined our results through the lens of place-based modelling we can now see the need to nuance our understanding of how these models function for the communities that generate them. The modelling engagement discussed here, and many others like it that we have conducted in multiple cases studies, are endowed with undoubtedly rich and unpredictable topologies. Many of the model elements have their own internal structure, and actors have horizons that can be subject to change. Actors can be constituted as being inside a central sphere of interest or outside this, characterised as 'other'. Within complex and shifting ecologies such as these, a 'door to the outside world' (Figure 9) represents more than simply 'common ground' over which actors can move. The LEGO models are far from being simple shared spaces, but display an array of shape-shifting and place-based modelling strategies.

Beyond this visible ecology of place and the structures that form them, there are other questions prompted by what is not visible. When considering which things are not depicted in the model, even though they may be referenced in the discussions of participants, we can ask why are they not modelled directly, and how this impacts on implicit 'horizons of understanding' and spaces of possible breakdown in the model. We saw in the IPTV model how dematerialised antagonists ('hackers') hover unseen over the model (and these are comically likened to Santa Claus). The many other ways in which the home is constructed as a situated place in the IPTV model automatically raises the issue of the home as a domain of anticipation and possible breakdown. Creative security methods highlight the fact that, as Winograd and Flores say, 'We are engaged in an activity of interpretation that creates both possibilities and blindness' (1986, p. 178). This is a blindness produced by an extended process of engagement and involvement with a community: 'Our view is limited to what can be expressed in the terms we have adopted. This is not a flaw to be avoided in thinking - on the contrary, it necessary and inescapable' (p. 97). The three points of interest introduced at the outset help researchers to work creatively with a community to see and work creatively with these necessary possibilities and blindnesses. The place-based ontologies of the group were visualised in the heat map of the IPTV model (Figure 8). Many other kinds of observations could be mapped onto their ontology in the same way - reversals of perspective, changes in horizons, spaces of potential breakdown, for example.

The IPTV participants depicted in their model how networks of resilience could be built up in the community with 'soft' human interventions - the knock on the door by a friendly advisor. The model demonstrates a principle of pluralistic democracy that, as Mouffe says, 'to construct the "them" in such a way that it is no longer perceived as an enemy to be destroyed, but an "adversary"', and that 'an adversary is an enemy, but a legitimate enemy, one with whom we have some common ground' (Mouffe, 2000, p. 15), and that 'the opponent should be considered not as an enemy to be destroyed, but as an adversary whose existence is legitimate and must be tolerated' (Mouffe, 1993, p. 4). The model also demonstrates how 'there can only be an identity when it is constructed as difference and that any social objectivity is constituted through acts of power' (Mouffe, 2009, p. 550). This is much as we have seen in the cases of the hacker and the bank and government. The modelling process appears to help participants to establish what the 'homeomorphic' or functional equivalents of any given concept are for a particular community (Panikkar, 1982, p. 81-82). In this case, the spoken of but unseen Santa Claus figure, not tied to any particular place or location but floating above these, becomes the equivalent to the notion of an external and dissociated antagonist.

Conclusion

An extensive process of engagement requires a level of experimentation and of dwelling with a community around the matters that concern them, as Escobar says. In this way, the above questions can be identified and pushed further, asking 'Why?' at each stage. This pushes at the edges of the spaces of possible breakdown, simultaneously narrowing down and extending the open-ended discussion of how a community constitutes and designs itself over a particular place, space and time. As Escobar notes, this process of developing an open-ended enquiry may require dwelling on a 'disharmony' presented by participants, but as the excerpts from our modelling interactions show, creative security methods dwell on disharmony by facilitating a playful 'space of confrontation' or agonistic contestation. The methods we have described, although viable as they are, could be extended into other forms of engagement suitable for working with a greater range of cultures and perspectives. The current method requires groups of participants to summarise their models for other groups (in engagements with larger numbers of people). This provides the basis for a 'conflictual consensus' or 'dissensus' to become the norm for the way that our engagements are framed. As Mouffe says, the notion of a community converging 'on one single model' without a considered view of how to take account of differing political interpretations runs counter to agonistic pluralism (Mouffe, 2009, p. 552). Extending the method and also the way it is framed would also be an opportunity to look at how public space is 'striated' in different ways for different people. As it stands, the method can absorb further aspects of 'critical making' - where there is a 'politicization of the artifact through the process of defining function and form' (DiSalvo, 2014, p. 97). This is of course a continuing process of evolving methods. The analysis of participatory data given here, is we hope a step towards resolving an outstanding issue: 'we are still in need of descriptive and analytic methods for making sense of and communicating the meaning and consequence of these endeavors' (DiSalvo, 2014, p. 104).

Processes of change are discussed in the context of the problematics of participatory design research by Keshavarz and Mazé, who foreground the contention that consensus cannot be reconciled with change, particularly where oppressive norms are in place (Keshavarz and Mazé, 2013, p. 9). Rather than achieving change through the rhetoric of consensus, the authors consider Mouffe's concept of 'agonistic pluralism' (Mouffe, 2009) and Rancière's 'dissensus' in order to allow for the 'presentation of conflicts between interest, opinions and ideas' within participatory design (Keshavarz and Mazé, 2013, p. 11). This is achieved by framing research as 'in-disciplinary' as opposed to interdisciplinary, so that no one imposes their 'voice, knowledge or discipline on the shared space of action/reaction' (Keshavarz and Mazé, 2013, p. 17).

Given the dominance of technical approaches to security and the tendency of the security industry to want to maximise profit from risk management business opportunities (Amoore, 2014, p. 6), it is difficult to imagine a shared space in information security in which the disciplinary expertise of security practitioners is not imposed. However, in prototyping the agonistic but creative approach described here, we have made some initial steps towards understanding and practicing security while using the terms, horizons, and ontologies of participants - rather than of security professionals. Our approach is to draw out of participants the relationships, practices, knowledges and associated ways of being that can be developed upon in order for a community to build up its strength and resilience, including relationships of trust. Creative security engagements seek to unseat a dominant model and disciplinary discourse with new understandings of security that are less hierarchical than current dominant approaches that have been conditioned by technical security alone.

Agonistic spaces of interaction have great transformative potential, and can capture the richer experiential, dimensional and agonistic picture. By asking fundamental questions during engagements such as 'Security for whom?', a space is opened up in which 'claims and voices of marginal actors can grow stronger' (Hillgren *et al.*, 2016, p. 97). Not discussed here are the potential benefits that creative security methods can have in determining what it means for a community to have collective wellbeing, or *Vivir Bien* (Escobar, 2012, p. 49). Our approach augments the notion of 'positive security', an enabling a collectivity with the *freedom to* - to pursue and exercise rights, and to follow matters of concern and interest (McSweeney, 1999). This is contrasted with negative conceptions of security, which are centred on prevention of threat - *freedom from*. The potentially transformative power of our approach is to bring to this a participatory dimension that constructs breakdowns as a way 'to identify the affirmative dimension of contestation' and of agonism (Honig, 1993, p. 15). This rests in bringing forward a 'multiplicity of voices' as Mouffe says, and the possibility of accepting a new paradigm on the basis of this, leading to 'a sort of conversion' through having seen it being made visible and manifest (Mouffe, 1993, p. 17). Beyond this, place-based modelling is also able to represent how the ontological security of actors is reproduced through routines carried out recursively and reciprocally across space and time. As Giddens says, 'routinization is vital to the psychological mechanisms whereby a sense of trust or ontological security in the daily activities of social life' is gained (Giddens, 1984, p. xxiii).

The Wannacry ransomware attack, discussed at the beginning of this paper, caused the widespread inability of NHS staff to carry on their daily functions, such as knowing which patients are booked for appointments and when they are due to arrive. Everyday routines and practices being disrupted in this way means that the attention of staff is drawn into managing the apparatus of communication itself, into its 'unreadiness-to-hand', or breakdown. This can help us to look more closely at the things that breakdown reveals, and help prevent, minimise and repair the damage caused by such attacks - attacks on trust and human security (as opposed to technical security). The creative security engagement method we have outlined here is concerned with showing how security effects everyone, and with democratising the process of designing securities with and for communities. The impact of the approach can perhaps best be measured in terms of how the conversation about security is conducted. This can be a rich agonistic dialogue between communities, permitting more than one understanding of security. This, in and of itself, strengthens security since it moves participants beyond a necessarily impoverished monocultural concept of security.

References

ADTOOL. 2018. Available at: http://satoss.uni.lu/projects/adt2p/adtool/ Accessed on: February 8, 2018.

AMOORE, L. 2013. *The politics of possibility: Risk and security beyond probability*. Durham, Duke University Press, 232 p.

ANTCONC. 2013. Build 3.5.2. Available at: http://www.laurenceanthony.net/software/antconc/ Accessed on: February 8, 2018.

BINDER, T.; DE MICHELIS, G.; EHN, P.; JACUCCI, G.; LINDE, P.; WAGNER, I. 2011. *Design things*. Cambridge, MIT Press, 256 p.

BJÖRGVINSSON, E.; EHN, P.; HILLGREN, P.A. 2012. Agonistic participatory design: working with marginalised social movements. *CoDesign*, **8**(2-3):127-144. https://doi.org/10.1080/15710882.2012.672577

BÜRGI, P.T.; JACOBS, C.D.; ROOS, J. 2005. From metaphor to practice: in the crafting of strategy. *Journal of Management Inquiry*, **14**(1):78-94. https://doi.org/10.1177/1056492604270802

BÜRGI, P.T.; ROOS, J. 2003. Images of strategy. *European Management Journal*, **21**(1):69-78. https://doi.org/10.1016/S0263-2373(02)00153-6

CANTONI, L.; FARÉ, M.; FRICK, E. 2011. *User Requirements with Lego.* Università della Svizzera Italiana (University of Lugano, Switzerland), Faculty of Communication Sciences: webatelier.net and NewMinE Lab. Available at: http://www.webatelier.net/lego-url-user-requirements Accessed on: December 15, 2017.

COLES-KEMP, L.; HANSEN, R.R. 2017, July. Walking the line: The everyday security ties that bind. *In:* T. TRYFONAS, (ed.), *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Berlin, Heidelberg, Springer, p. 464-480.

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD (CSTB). 1991. *Computers at Risk: Safe Computing in the Information Age*. Washington, DC, National Academy Press, 320 p.

CROPLEY, D.H. 2010. *The dark side of creativity: a differentiated model. In:* CROPLEY, D.H.; CROPLEY, A.J.; KAUFMAN, J.C.; RUNCO, M.A. (eds.), *The Dark Side of Creativity.* Cambridge, Cambridge University Press, p. 360-373.

DISALVO, C. 2010. Design, Democracy and Agonistic Pluralism. *In:* D. DURLING (ed.), *Design and Complexity. Proceedings of the Design Research Society Conference.* Montreal, Université de

Montréal, p. 366-371.

DISALVO, C. 2012. *Adversarial design*. Cambridge, MIT Press, 168 p.

DISALVO, C. 2014. Critical Making as Materializing the Politics of Design. *The Information Society*, **30**: 96-105. https://doi.org/10.1080/01972243.2014.875770

DUNPHY, P.; VINES, J.; COLES-KEMP, L.; CLARKE, R.; VLACHOKYYRIAKOS, V.; WRIGHT, P.; MCCARTHY, J.; OLIVIER, P. 2014. Understanding the experience-centeredness of privacy and security technologies. *In:* K. BEZNOSOV, A. SOMAYAJI, T. LONGSTAFF, P. VAN OORSCHOT (eds.), *Proceedings 2014 Workshop on New Security Paradigms Workshop*. New York, ACM, p. 83-94. Available at: https://dl.acm.org/citation.cfm?doid=2683467.2683475

ELAN. 2017. Nijmegen: Max Planck Institute for Psycholinguistics. Version 5.0.0-beta. Available at: https://tla.mpi.nl/tools/tla-tools/elan/ Accessed on: April 18, 2017.

ESCOBAR, A. 2012. Notes on the Ontology of Design (Draft). Available at: http://sawyerseminar.ucdavis.edu/files/2012/12/ESCOBAR_Notes-on-the-Ontology-of-Design-Parts-I-II-_-III.pdf Accessed on: December 15, 2017.

ESCOBAR, A. 2017. Response: Design for/by [and from] the 'global South.' *Design Philosophy Papers*, **15**(1):39-49. https://doi.org/10.1080/14487136.2017.1301016

GIDDENS, A. 1984. *The constitution of society: Outline of the theory of structuration*. Berkeley, University of California Press, 402 p.

HANSEN, L.; NISSENBAUM, H. 2009. Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, **53**(4):1155-1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

HARAWAY, D. 1988. Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective. *Feminist Studies*, **14**(3):575-599. https://doi.org/10.2307/3178066

HEATH, C.P.R.; COLES-KEMP, L. 2017. *The Internet of Things: Creating the necessary conditions for secure by default. Special Report for DCMS Working Group on Consumerism and the Internet of Things.* London, Information Security Group, Royal Holloway University of London, 37 p.

HEATH, C.P.R.; COLES-KEMP, L.; HALL P.A. 2014. Logical LEGO? Co-constructed perspectives on service design. *In:* M. LAASKO; K. EKMAN (eds.), *Proceedings of NordDesign 2014 Conference*. The Design Factory, Swinburne Institute of Technology, Melbourne, Australia. Aalto, Design Society & Aalto University, p. 416-425.

HEATH, C.P.R. 2014. *Drawing out interaction: Lines around shared space*. London, UK. PhD thesis. Queen Mary, University of London, 382 p. Available at: https://qmro.qmul.ac.uk/jspui/handle/123456789/8817 Accessed on: June 6, 2017.

HILLGREN, P.A.; SERAVALLI, A.; ERIKSEN, M.A. 2016. Counter-hegemonic practices; dynamic interplay between agonism, commoning and strategic design. *Strategic Design Research Journal*, **9**(2):89-99. https://doi.org/10.4013/sdrj.2016.92.04

HONIG, B. 1993. *Political theory and the displacement of politics*. Ithaca, Cornell University Press, 304 p.

INTERACTOR. 2018. Available at: http://interactor.co/ Accessed on: May 15, 2018.

KESHAVARZ, M.; MAZE, R. 2013. Design and Dissensus: Framing and Staging Participation in Design Research. *Design Philosophy Papers*, **11**(1):7-29. https://doi.org/10.2752/089279313X13968799815994

LANKHORST, M.M.; PROPER, H.A.; JONKERS, H. 2009. The architecture of the Archimate language. *In:* I. BIDER; T. HALPIN; J. KROGSTIE; S. NURCAN; E. PROPER; R. SCHMIDT; P. SOFFER; S. WRYCZA (eds.), *Enterprise, Business-Process and Information Systems Modeling*. Berlin, Heidelberg, Springer, p. 367-380. https://doi.org/10.1007/978-3-642-01862-6_30

MANDAL, S.; LIM, E.P. 2008, May. Second life: Limits of creativity or cyber threat? *In:* IEEE Conference on Technologies for Homeland Security, Boston, 2008. *Proceedings*, IEEE, p. 498-503.

MCSWEENEY, B. 1999. *Security, identity and interests: a sociology of international relations*. Cambridge, Cambridge University Press, vol. 69, 256 p. https://doi.org/10.1017/CBO9780511491559

EHRENFIELD, J.M. 2017. Wannacry, cybersecurity and health information technology: A time to act. *Journal of Medical Systems*, **41**(7):104.

MOUFFE, C. 1993. *The Return of the Political*. London/New York, Verso, 170 p.

MOUFFE, C. 2000. Deliberative democracy or agonistic pluralism. Available at: http://www.ssoar.info/ssoar/handle/document/24654. Accessed on: December 15, 2017.

MOUFFE, C. 2009. Democracy in a multipolar world. *Millennium*, **37**(3):549-561. https://doi.org/10.1177/0305829809103232

PANIKKAR, R. 1982. Is the notion of human rights a Western concept? *Diogenes*, **30**(120):75-102. https://doi.org/10.1177/039219218203012005

ROOS, J.; VICTOR, B.; STATLER, M. 2004. Playing seriously with strategy. *Long Range Planning*, **37**(6):549-568. https://doi.org/10.1016/j.lrp.2004.09.005

SCHNEIER, B. 1999. Attack trees. *Dr. Dobb's Journal*, **24**(12):21-29.

SCHULZ, K.P.; GEITHNER, S. 2011. The development of shared understandings and innovation through metaphorical methods such as LEGO Serious Play. *In:* International Conference on Organizational Learning, Knowledge and Capabilities, Hull, 2011. *Proceedings...* Hull University Business School. 12 p.

STATEN, H. 1986. *Wittgenstein and Derrida*. Lincoln/London, University of Nebraska Press, 184 p.

TRESPASS. European Commission's Seventh Framework Programme (FP7), Grant No. 318003. 2013-2017. Available at: http://www.trespass-project.eu/. Accessed on: December 15, 2017.

WINOGRAD, T.; FLORES, F., 1986. *Understanding computers and cognition: A new foundation for design.* Bristol, Intellect Books, 224 p.

Submitted on December 15, 2017
Accepted on May 17, 2018